AP 2135
JZW

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS
AND INTERFERENCES

OIPE
MAR 2 4 2005

Patent Application

Inventors:	**Satish Bommareddy**
	Srinivas Chaganty
	Makarand Kale

Case No.: **CyberIQ M-8403**

Serial No.: **09/540,238**   Group Art Unit: **2135**

Filing Date: **April 1, 2000**

Examiner: **Leynna A. Ha**

Title: **Firewall Pooling In a Network Flowswitch**

Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

SIR:

<u>APPLICANTS'/APPELLANTS' APPEAL BRIEF</u>

This is an appeal from anticipation and obviousness rejections of claims of an application relating to fault-tolerance in a network, achieved through a pool of firewalls. Appellants request that the Board reverse the rejection as erroneous.

TABLE OF CONTENTS

Real Party in Interest

Related Appeals and Interferences

Status of Claims

Status of Amendments

Summary of Claimed Subject Matter
    Claim 1
    Claim 16
    Claim 23
    Claim 40
    Claim 47
    Claim 57

Grounds of Rejection to be Reviewed or Appeal

Arguments
    A. The Section 102(e) rejection over Coile et al.
        1. The disclosure of Coile et al.
        2. The grounds of the rejection.
        3. The Examiner is wrong: the network devices of Coile et al. in
            fact do swap their MAC addresses with each other.

    B. The Section 103(a) rejection over Coile et al. in view of Belville et al.
        1. The disclosure of Belville et al.
        2. The grounds of the rejection.
        3. Belville et al. do not make up for the failure of Coile et al. to
            teach the claimed invention.

Conclusion

Claim Appendix

Evidence Appendices
    Appendix A – Final Office Action

    Appendix B – Coile et al.

    Appendix C – Belville et al.

Related Proceedings Appendix (none)

REAL PARTY IN INTEREST

The real party in interest is Avaya Technology Corp., the assignee of the above-identified application, as evidenced by the Assignment from the inventors to CyberIQ Systems recorded on Reel 011205, Frame 0352, by an assignment from CyberIQ Systems to Avaya, Inc. recorded on Reel 012698, Frame 0735, and by assignment from Avaya, Inc. to Avaya Technology Corp. recorded on Reel 012698, Frame 0673.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF CLAIMS

Claims 1-63 are pending.

Claims 1-7, 14-19, 23-30, and 37-63 stand rejected under 35 U.S.C. §102(e) over U.S. patent number 6,108,300 (Coile et al.).

Claims 8-13, 20-22, and 31-36 stand rejected under 35 U.S.C. §103(a) over Coile et al. in view of U.S. patent number 5,828,833 (Belville et al.).

The appealed claims are claims 1-63.

STATUS OF AMENDMENTS

No amendments were filed subsequent to final rejection.

CLAIMED SUBJECT MATTER

The inventor has invented a way of providing protection against failure of a firewall in a network (300 of Fig. 3) by pooling a plurality of firewalls (104 and 202 in Fig. 3), detecting a failure of one of the firewalls, and automatically sending packets that were addressed to the failed firewall to one of the other firewalls (page 3, lines 25-28). Significantly, each firewall has its own media access control (MAC) address, and when a firewall fails, the MAC address in all packets addressed to the failed firewall is replaced with the MAC address of another, the replacement, firewall, so that thereafter

the packets are sent to the replacement firewall instead of the failed firewall (page 5, lines 18-22).

The replacement of the MAC addresses in packets is transparent and non-intrusive to the network and to the firewalls. Advantageously, therefore, there is substantially no need to make non-standard reconfigurations to support firewall fault-tolerance (page 5, lines 26-29).

Claim 1

In addition to the firewalls, the network includes at least one server (106 and 108 in Fig. 3) and at least one flowswitch (302 in Fig. 3) (page 9, lines 17-18). When the flowswitch detects (401 in Fig. 4) that a firewall has failed (page 10, line 20, or page 10, line 31, to page 11, line 1), it monitors traffic from the servers to the failed firewall (page 11, lines 1-12). When it detects (405 in Fig. 4) a packet having the MAC address of the failed firewall, the flowswitch translates (405 in Fig. 4) the packet's MAC address from the MAC address of the failed firewall to the MAC address of a functional firewall, and then relays the modified packet to the functional firewall (page 11, lines 15-22).

Claim 16

Means for detecting an occurrence of a failed firewall correspond to a flowswitch (802 in Fig. 7, or 11 or 14 in Fig. 9A) performing the function of block 9 of Fig. 8A or of block 21 of Fig. 9C) (page 18, line 25, to page 19, line 1, or page 20, lines 25-26). Means for detecting a packet correspond to the flowswitch performing the function of blocks 910 and 912 of Fig. 8B (page 17, lines 2-14). Means for changing a MAC address correspond to the flowswitch performing the function of block 916 of Fig. 8B or of block 23 of Fig. 9C (page 19, lines 13-24, or page 20, lines 28-30). Means for relaying the packet correspond to the flowswitch performing the function of block 24 of Fig. 9C (page 20, line 31, to page 21, line 3).

Claim 23

A network (300 in Fig. 3) has a firewall fault-tolerance (page 3, lines 25-26). The network is configured to be coupled to a network backbone (102 in Fig. 3). The network couples a switch circuit (302 in Fig. 3), a first firewall (104 in Fig. 3), a second firewall (202 in Fig. 3), and a server (106 or 108 in Fig. 3). Each firewall is coupled to the switch circuit and to the network backbone (page 9, lines 6-9), and has its own fixed media access control (MAC) address (page 11, lines 16-22). The server is coupled to the switch circuit (page 11, lines 17-18) and is configured to detect (401 in Fig. 4) when the first firewall fails (page 10, line 15, to page 11, line 6). The switch circuit is further configured to monitor packets sent by the server to the first firewall (page 11, lines 11-12), and to change (405 in Fig. 4) the fixed MAC address of the first firewall in the packet to the fixed MAC address of the second firewall (page 11, lines 12-22).

Claim 40

A method of providing fault-tolerance (page 3, lines 25-26) in a network (300 in Fig. 3) that includes a plurality of firewalls (13A-13N in Fig. 9A), each having a different fixed media access control (MAC) address (page 11, lines 16-22) comprises the following steps: Generating (25 in Fig. 9D) a request message on a first side of a first firewall in the plurality of firewalls (page 21, lines 4-7). Sending (26 in Fig. 9D) the request message through the first firewall to a second side of the first firewall (page 21, lines 7-9). Processing (28 in Fig. 9D) an absence (27 in Fig. 9D) of a reply from the second side to the request message as a failure of the first firewall (page 21, lines 9-12), including replacing (23 in Fig. 9C), in a packet, the fixed MAC address of the first firewall with the fixed MAC address of a second firewall of the plurality of firewalls (page 20, line 25, to page 21, line 1).

Claim 47

A fault tolerant (page 3, lines 15-26) network (10 in Fig. 9A) comprises a first switch circuit (11 in Fig. 9A), a second switch circuit (14 in Fig. 9A), and a plurality of firewalls (13A-13N in Fig. 9A) (page 19, lines 24-26). The

firewalls each have a different fixed media access control (MAC) address (page 11, lines 16-22). Each firewall is coupled to the first switch circuit by a first medium (12A, ...12N) that is not shared with another firewall in the plurality of firewalls (page 20, lines 3-4). Likewise, each firewall is coupled to the second switch circuit by a second medium that is not shared with another firewall in the plurality of firewalls (see Fig. 9A). A switch circuit of the first and the second switch circuits responds to a first firewall of the plurality of firewalls being functional by sending (block 22 of Fig. 9C) a first packet that has the fixed MAC address of the first firewall and is received by said switch circuit to the first firewall (page 20, lines 25-28). The switch circuit responds to a failure of the first firewall by replacing (block 23 of Fig. 9C) in a second packet received by said switch circuit the fixed MAC address of the first firewall with the fixed MAC address of a functional second firewall of the plurality of firewalls and sending (block 24 of Fig. 9C) the second packet with the replaced MAC address to the second firewall (page 20, line 28, to page 21, line 1).

Claim 57

A method of providing fault-tolerance (page 3, lines 25-26) in a network (300 in Fig. 3) that includes a plurality of firewalls (13A-13N in Fig. 9A) each having a different fixed media access control (MAC) address (page 11, line 16-22) comprises the following steps: Detecting (block 21 in Fig. 9C) a failure of a first firewall in the plurality of firewalls (page 20, lines 25-26). Replacing (block 23 of Fig. 9C), in a packet, the fixed MAC address of the first firewall with the fixed MAC address of a second firewall of the plurality of firewalls in response to the failure (page 20, line 28, to page 21, line 1).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL.

    A. Claims 1-7, 14-19, 23-30, and 37-63 stand rejected under 35 U.S.C. §102(e) over US patent no. 6,108,300 (Coile et al.).

    B. Claims 8-13, 20-22, and 31-36 stand rejected under 35 U.S.C. §103(a) over Coile et al. in view of U.S. patent no. 5,828,853 (Belville et al.).

ARGUMENT

A. The Section 102(e) rejection over Coile et al.

1. The disclosure of Coile et al.

Coile et al. (Appendix B of Exhibit Appendices) disclose an arrangement for transferring a network function from a primary network device to a backup network device. When the backup device detects that the primary device has failed, the backup device takes on the MAC and IP addresses of the failed network device, while the failed network device takes on the MAC and IP addresses of the formerly-backup device (Abstract, col. 1, lines 37-39, col. 7, lines 10-27). In other words, the two devices swap their MAC and IP addresses with each other.

2. The basis of the rejection.

The appealed claims require that individual firewalls have different and fixed MAC addresses, and that, upon failure of a firewall, the MAC address of the failed firewall is changed in packets to the MAC address of a functional firewall. In other words, MAC addresses of firewalls are swapped in packets, and not between firewalls. This is in direct contrast to Coile et al., where the two network devices swap their MAC addresses with each other.

Nevertheless, the Examiner purported to find anticipatory teaching in Coile et al. (see, e.g., Final Office Action mailed on September 22, 2004 (Appendix A of Evidence Appendices), page 3, line 19, to page 4, line 8). In responding to applicants' assertion that Coile et al. and the claimed invention are substantially contrary to each other because the network devices of Coile et al. swap their MAC addresses with each other, the Examiner stated that the network devices of Coile et al. in fact do not swap their MAC addresses, because "it would not be logical" (Id. at p. 24).

3. The Examiner is wrong; the network devices of Coile et al. in fact do swap their MAC addresses with each other.

Applicants respectfully assert that the Examiner is wrong. Coile et al. explicitly state that the two devices do swap their MAC addresses with each other. For example, col. 1, lines 38-40 state that "The backup network device takes over the active MAC and IP addresses from the failed network device..." Col. 6, lines 11-13 state that "the active MAC address is adopted by the active network device and is therefore not assigned to only one device." Col. 7, lines 17-23 state that, if the formerly-active device still responded to its former MAC address, a switch might not be able to properly learn that the active MAC address has changed; "this is avoided and the former active device moves to the standby IP and MAC address." Col. 10, lines 34-49 state that "when the active and standby network devices change state, they also change MAC address and IP addresses...", "the devices have traded IP and MAC addresses", "the active MAC address has moved over to...the backup device, which is now active", and "the primary device...begin[s] using the MAC and IP addresses of the standby device" (emphasis added). And, col. 12, lines 15-20 state that "The backup device assumes the MAC address and the IP address of the active device [, and] the formerly active device...assumes the standby MAC address and standby IP address."

Furthermore, col. 1, lines 36-37 state that this swapping of the MAC and IP addresses between the failed active device and the standby device eliminates "the need for other network devices to change the MAC or IP address to which they are directing packets." Correspondingly, col. 12, lines 41-44 state that "Because the backup device assumes the active MAC address, it is not even necessary for each of the clients to ARP to find out a new MAC address...to which the client is attempting to connect." These statements would not be true if, as the Examiner asserts, the two devices did not swap their MAC addresses.

It should therefore be amply evident that the two network devices in Coile et al. do swap their MAC addresses with each other upon the failure of

one of them, and consequently that the teaching of Coile et al. is directly contrary to the recitations of applicants' claims.

B. The Section 103(a) rejection over Coile et al. in view of Belville et al.

1. The teaching of Belville et al.

Belville et al. (Appendix C of Exhibit Appendices) disclose an arrangement for allowing remote procedure calls from an application server to pass through a network firewall (Abstract). A firewall application running on a firewall server is multithreaded: two threads register and unregister application servers for making remote procedure calls through the firewall, and a clean-up thread pings application servers and other firewall applications to make sure that they are still operational (col. 6, lines 22-55).

2. The basis for the rejection.

The Examiner referenced Bellville et al. for teaching proper recovery from failure of a firewall, and teaching a firewall application that includes a clean-up thread that periodically pings servers to determine if the servers and firewalls are still present and operable (see, e.g., Appendix A of Exhibit Appendices at page 14, lines 19-23).

3. Belville at al. do not make up for the failure of Coile et al. to teach the claimed invention.

The teaching of Bellville et al. do not supplement the teachings of Coile et al. in any way that is relevant to the basic invention claimed in the appealed claims. Consequently, the combined teachings of Coile et al. and Bellville et al. do not render the claimed invention unpatentable.
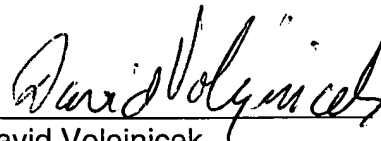
CONCLUSION

For all the reasons given above, applicants respectfully assert that the Sections 102(e) and 103(a) rejections of all of the claims are not well founded. Applicants therefore respectfully request that the rejections of the appealed claims be reversed.

Respectfully submitted,

**Satish Bommareddy
Srinivas Chaganty
Makarand Kale**

By _David Volejnicek_
. David Volejnicek
Corporate Counsel
Reg. No. 29355
303-538-4154

Date: _March 21, 2005_
Avaya Inc.
Docket Administrator
307 Middletown-Lincroft Road
Room 1N-391
Lincroft, NJ 07738

THE APPEALED CLAIMS

 1. A method for providing firewall fault-tolerance in a network, the network including a plurality of firewalls, at least one server and at least
4 one network flowswitch, the method comprising:
5 detecting in the network flowswitch an occurrence of a failed
6 firewall of the plurality of firewalls each having a different fixed media
7 access control (MAC) address;
8 detecting in the network flowswitch a packet from the server
9 directed to the failed firewall after the occurrence of a failed firewall is
10 detected;
11 changing a MAC address of the packet to the fixed MAC
12 address of a functional firewall of the plurality of firewalls when the packet
13 is detected; and
14 relaying the packet to the functional firewall after the MAC
15 address of the packet is changed.

1 2. The method of claim 1 wherein the network comprises a
2 plurality of servers.

1 3. The method of claim 2 wherein relaying the packet to the
2 functional firewall comprises relaying the packet to the functional firewall
3 over a medium that is not shred with packets directed to other firewalls or
4 servers.

1 4. The method of claim 1 wherein said detecting an occurrence
2 of a failed firewall comprises sending a request to the plurality of firewalls,
3 wherein an absence of a response from a particular firewall of the plurality
4 of firewalls is indicative of a failure of the particular firewall.

1   5. The method of claim 1 wherein said detecting an occurrence
2   of a failed firewall comprises sending at least one Address Resolution
3   Protocol (ARP) request to each firewall of the plurality of firewalls, wherein
4   an absence of a reply to an ARP request from a particular firewall of the
5   plurality of firewalls is indicative of a failure of the particular firewall.

1   6. The method of claim 1 further comprising:
2   detecting an address resolution protocol (ARP) request from the
3   server to the failed firewall; and
4   responding to the ARP request with the fixed MAC address of
5   the functional firewall, whereby the server is configured to send
6   subsequent outbound packets with the fixed MAC address of the
7   functional firewall.

1   7. The method of claim 1 wherein said detecting an occurrence
2   of a failed firewall comprises sending ICMP echo packets to each firewall
3   of the plurality of firewalls and wherein an absence of a response from a
4   particular firewall of the plurality of firewalls during a predetermined
5   interval is indicative of a failure of the particular firewall.

1   8. The method of claim 1 further comprising:
2   detecting a recovery of the failed firewall, the failed firewall
3   becoming a recovered firewall; and
4   terminating said detecting a packet from the server directed to
5   the failed firewall when said failed firewall recovers.

1   9. The method of claim 8 further comprising waiting for a time-
2   out period to expire after said detecting when the failed firewall recovers.

1   10. The method of claim 9 wherein the time-out period is
2   greater than or equal to a time period needed for the recovered firewall to
3   learn routes to all known clients.

1   11. The method of claim 8 wherein said detecting a recovery of
2   the failed firewall comprises sending to the failed firewall a request, and a
3   response from the failed firewall is indicative of a recovery of the failed
4   firewall.

1   12. The method of claim 8 wherein said detecting a recovery of
2   the failed firewall comprises detecting a packet from the failed firewall in
3   response to a request.

1   13. The method of claim 8 wherein said detecting a recovery of
2   the failed firewall comprising sending ARP requests to each firewall of the
3   plurality of firewalls, wherein an occurrence of a reply to an ARP request
4   from the failed firewall is indicative of a recovery of the failed firewall.

1   14. The method of claim 1 wherein packets are transferred
2   between the server and a firewall of the plurality of firewalls through a
3   switch circuit.

1   15. The method of claim 14 wherein the switch circuit
2   comprises a switched Ethernet circuit.

1   16. An apparatus for providing firewall fault-tolerance in a
2   network, the network including a plurality of firewalls, at least one server
3   and at least one network flowswitch, the apparatus comprising:
4   means for detecting an occurrence of a failed firewall in the
5   plurality of firewalls each having a difference fixed media access control
6   (MAC) address;

7   means for detecting a packet from the server directed to the

8   failed firewall after the failed firewall is detected;

9   means for changing a MAC address of the packet to the fixed

10   MAC address of a functional firewall of the plurality of firewalls when the

11   packet is detected; and

12   means for relaying the packet to the functional firewall after the

13   MAC address of the packet is changed.

1   17.   The apparatus of claim 16 further comprising:

2   means for detecting an address resolution protocol (ARP)

3   request from the server to the failed firewall; and

4   means for responding to the ARP request with the fixed MAC

5   address of the functional firewall, wherein the server sends subsequent

6   outbound packets with the fixed MAC address of the functional firewall.

1   18.   The apparatus of claim 16 wherein said means for detecting

2   a failed firewall comprises means for transmitting a request to the plurality

3   of firewalls, wherein an absence of a reply from a particular firewall of the

4   plurality of firewalls is indicative of a failure of the particular firewall.

1   19.   The apparatus of claim 16 wherein said means for detecting

2   a failed firewall comprises means for sending ARP requests to each

3   firewall of the plurality of firewalls, wherein an absence of a reply to an

4   ARP request from a particular firewall of the plurality of firewalls is

5   indicative of a failure of the particular firewall.

1   20.   The apparatus of claim 16 further comprising:

2   means for detecting a recovery of the failed firewall, the failed

3   firewall becoming a recovered firewall; and

4   means for disabling said means for detecting a packet from the

5   server directed to the failed firewall when said failed firewall recovers.

1   21. The apparatus of claim 20 wherein said means for detecting

2   a recovery of the failed firewall comprises means for transmitting a request

3   to the plurality of firewalls, wherein a response from the failed firewall is

4   indicative of recovery of the failed firewall.

1   22. The apparatus of claim 16 wherein said means for detecting

2   a recovery of the failed firewall comprises means for sending ARP

3   requests to each firewall of the plurality of firewalls, wherein an occurrence

4   of a replay to an ARP request from the failed firewall is indicative of a

5   recovery of the failed firewall.

1   23. A network having firewall fault-tolerance, the network

2   configured to be coupled to a network backbone, the network comprising:

3   a switch circuit;

4   a first firewall coupled to said switch circuit and the network

5   backbone, said first firewall having a fixed media access control (MAC)

6   address;

7   a second firewall coupled to said switch circuit and the network

8   backbone, said second firewall having a fixed MAC address different from

9   the fixed MAC address of the first firewall; and

10   a server coupled to the switch circuit,

11   wherein the switch circuit is configured to detect when the first

12   firewall fails, the switch circuit being further configured to monitor packets

13   sent by the server to the first firewall and to change in the packet the fixed

14   MAC address of the first firewall to the fixed MAC address of the second

15   firewall.

1   24. The network of claim 23 further comprising a plurality of

2   servers, the plurality of servers including the server.

1   25. The network of claim 23 wherein the switch circuit is further

2   configured to relay the packet to the second firewall after changing the

3   fixed MAC address of the first firewall to the fixed MAC address of the

4   second firewall.

1   26. The network of claim 23 wherein the switch circuit is

2   configured to detect a failed firewall by transmitting a request to the first

3   and second firewalls, wherein an absence of a reply from a particular

4   firewall of the first and second firewalls is indicative of a failure of the

5   particular firewall.

1   27. The network of claim 23 wherein the switch circuit is

2   configured to detect a failed firewall by sending ARP requests to the first

3   and second firewalls, wherein an absence of a replay to an ARP request

4   from a particular firewall of the first and second of firewalls is indicative of

5   a failure of the particular firewall.

1   28. The network of claim 23 wherein the switch circuit is

2   configured to detect a failed firewall by sending ICMP echo requests to the

3   first and second firewalls, wherein an absence of a reply to an ICMP echo

4   request from a particular firewall of the first and second of firewalls is

5   indicative of a failure of the particular firewall.

1   29. The network of claim 23 wherein the switch circuit is

2   configured to detect a failed firewall by monitoring responses from the

3   firewalls to requests sent at predetermined intervals.

1   30. The network of claim 23 wherein the switch circuit is further

2   configured to:

3   detect an address resolution protocol (ARP) request from the

4   server to the first firewall; and

5   respond to the ARP request with the fixed MAC address of the

6   second firewall, whereby the server sends subsequent outbound packets

7   with the fixed MAC address of the second firewall.

1   31. The network of claim 23 wherein the switch circuit is further

2   configured to:

3   detect when the first firewall recovers; and

4   terminate monitoring for packets sent by the server to the first

5   firewall after the first firewall recovers.

1   32. The network of claim 31 wherein the switch circuit is further

2   configured to wait for a time-out period to expire after detecting when the

3   first firewall recovers.

1   33. The network of claim 32 wherein the time-out period is

2   greater than or equal to a time period needed for the recovered first

3   firewall to learn routes to all known clients.

1   34. The network of claim 31 wherein the switch circuit is

2   configured to detect a recovery of the failed firewall by transmitting a

3   request to the first and second firewalls, wherein receipt of a response

4   from the failed firewall is indicative of a recovery of the failed firewall.

1   35. The network of claim 31 wherein the switch circuit is

2   configured to detect a recovery of the failed firewall by sending ARP

3   requests to the first and second firewalls, wherein an occurrence of a reply

4   to an ARP request from the failed firewall is indicative of a recovery of the

5   failed firewall.

1   36. The network of claim 31 wherein the switch circuit is

2   configured to detect a recovery of the failed firewall by sending ICMP echo

3   requests to the first and second firewalls, wherein an occurrence of a reply

4   to an ICMP echo request from the failed firewall is indicative of a recovery

5   of the failed firewall.

1   37. The network of claim 23 wherein packets are transferred

2   between the server and the first firewall through the switch circuit, and

3   between the server and the second firewall through the switch circuit.

1   38. The network of claim 36 wherein the switch circuit is

2   configured to provide full-duplex communication between the first firewall

3   and the server.

1   39. The network of claim 36 wherein the switch circuit

2   comprises a switched Ethernet circuit.

1   40. A method for providing fault-tolerance in a network, the

2   network including a plurality of firewalls each having a different fixed

3   media access control (MAC) address, the method comprising:

4   generating a request message on a first side of a first firewall in

5   the plurality of firewalls;

6   sending the request message through the first firewall to a

7   second side of the first firewall; and

8   processing an absence of a reply from the second side to the

9   requst message as a failure of the first firewall, including

10   replacing, in a packet, the fixed MAC address of the first firewall

11   with the fixed MAC address of a second firewall of the plurality of firewalls.

1   41. The method of claim 40 further comprising:

2   maintaining in a first memory on said first side a first functional

3   status for each firewall;

4   maintaining in a second memory on said second side a second

5   functional status for each firewall; and

6   wherein said first functional status is identical to said second

7   functional status.

1   42. The method of claim 41 further comprising:

2   maintaining session information in a firewall for each session

3   between computers separated by the firewall.

1   43. The method of claim 40 further comprising:

2   sending the request message through the first firewall to a third

3   side of the first firewall; and

4   processing an absence of a reply from the third side to the

5   request message as a failure of the first firewall.

1   44. The method of claim 40 wherein:

2   the generating, sending and processing are performed in a

3   switch circuit.

1   45. The method of claim 40 further comprising:

2   performing Network Address Translation (NAT) in the first

3   firewall; and

4   adding a rule in the first firewall to maintain unchanged an

5   internet protocol (IP) address of a source of the request message.

1   46. The method of claim 40 further comprising:

2   receiving a request on a port; and

3   sending a reply on said port.

1   47. A network having fault-tolerance, the network comprising:

2   a first switch circuit;

3   a second switch circuit; and

4   a plurality of firewalls each having a different fixed media access

5   control (MAC) address, the plurality of firewalls being coupled to each of

6   the first switch circuit and the second switch circuit, each firewall being

7   coupled to the first switch circuit by a first medium that is not shared with

8   another firewall in the plurality of firewalls and each firewall being coupled

9   to the second switch circuit by a second medium that is not shared with

10   another firewall in the plurality of firewalls; wherein

11   a switch circuit of the first and the second switch circuits

12   responds to a first firewall of the plurality of firewalls being functional by

13   sending a first packet that has the fixed MAC address of the first fiewall

14   and is received by said switch circuit to the first firewall, and responds to a

15   failure of the first firewall by replacing in a second packet received by said

16   switch circuit the fixed MAC address of the first firewall with the fixed MAC

17   address of a functional second firewall of the plurality of firewalls and

18   sending the second packet with the replaced MAC address to the second

19   firewall.

1   48. The network of claim 47 further comprising:

2   a plurality of first computers, each first computer being coupled

3   to the first switch circuit, each first computer being configured with the

4   media access control (MAC) address of the first firewall, the first firewall

5   being a default gateway for transferring packets outside the network.

1   49. The network of claim 48 further comprising:

2   a plurality of second computers, each second computer being

3   coupled to the second switch circuit, each second computer being

4   configured with the MAC address of the first firewall, the first firewall being

5   a default gateway for transferring packets inside the network.

1   50. The network of claim 47 further comprising:

2   a plurality of routers coupled to the second switch circuit.

1   51. The network of claim 47 wherein each of the first switch

2   circuit and the second switch circuit comprises:

3   a first storage element encoded with a list of the plurality of

4   firewalls; and

5   a second storage element encoded with an ~~identify~~ identity of a

6   firewall in the plurality as a replacement firewall for any other firewall in the

7   plurality that has failed.

1   52. The network of claim 47 wherein:

2   each of the first switch circuit and the second switch circuit is

3   configured to send a request message to the other of the first switch circuit

4   and the second switch circuit; and

5   each of the first switch circuit and the second switch circuit is

6   configured to treat absence of a response to the request message as a

7   failure of a firewall through which the request message was sent.

1   53. The network of claim 52 wherein:

2   the request message conforms to an internet protocol selected

3   from the group consisting of:

4   (a) ping;

5   (b) address resolution protocol (ARP); and

6   (c) internet message control protocol (ICMP).

1   54. The network of claim 47 wherein:

2   the first switch circuit transfers a plurality of packets to the first

3   firewall through a first medium without changing any portion of any packet

4   in the plurality of packets while the first firewall is functional.

1   55. The network of claim 47 wherein:

2   the switch circuit replaces in each received packet the fixed

3   MAC address of the first firewall with the MAC address of the second

4   firewall and transfers each modified packet to the second firewall only

5   while the first firewall is nonfunctional.

1   56. The network of claim 47 wherein each switch circuit

2   comprises a switched Ethernet circuit.

1   57. A method of providing fault-tolerance in a network, the

2   network including a plurality of firewalls each having a different fixed

3   media access control (MAC) address, the method comprising:

4   detecting a failure of a first firewall in the plurality of firewalls;

5   and

6   replacing, in a packet, the fixed MAC address of the first firewall

7   with the fixed MAC address of a second firewall in the plurality of firewalls

8   in response to the failure.

1   58. The method of claim 57 wherein:

2   the detecting is performed in a switch circuit.

1   59. The method of claim 57 further comprising:

2   receiving the packet after detecting the failure and prior to the

3   replacing.

1   60. The method of claim 57 further comprising:

2   transferring a plurality of packets other than the packet, between

3   a host and a firewall in the plurality of firewalls through a switch circuit.

1   61. The method of claim 60 wherein:

2   each of the packets contains a first internet protocol(IP address;

3   and

4   the method does not change the first IP address during

5   transferring of the packets to any of the firewalls.

1   62. The method of claim 61 wherein:

2   each of the firewalls has a first side and a second side; and

3   each of the firewalls has the first IP address on the first side and

4   a second IP address on the second side.

1   63. The method of claim 61 wherein:

the method does not change the MAC address of any of the

packets during the transferring, until the detecting of failure.

SUE 11-22-04

United States Patent and Trademark Office

Cyber Id M-8403

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/540,238	04/01/2000	Srinivas Chaganty	M-8403 US	9955

7590 09/22/2004

David Volejnicek, Esq.
Avaya Inc.
307 Middletown-Lincroft Road
Room 1N-391
LINCROFT, NJ 07738

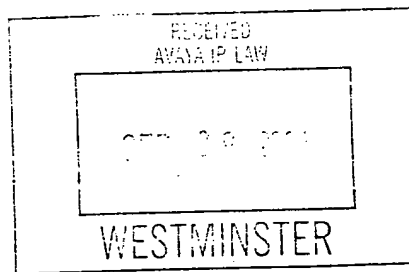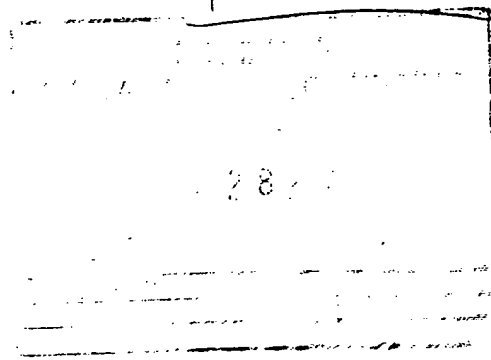| EXAMINER |
|---|
| HA, LEYNNA A |

ART UNIT	PAPER NUMBER
2135	

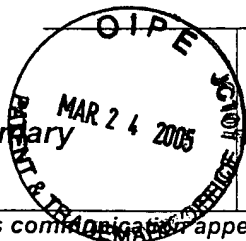DATE MAILED: 09/22/2004

OIPE
MAR 2 4 2005
PATENT & TRADEMARK

Final

Please find below and/or attached an Office communication concerning this application or proceeding.

Due 12-22-04

checked
9-29-04
JRH

28

RECEIVED
AVAYA IP LAW

WESTMINSTER

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-63* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-63* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____ .

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)	4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) ☐ Notice of Informal Patent Application (PTO-152)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .	6) ☐ Other:

DETAILED ACTION

1. Claims 1-63 have been re-examined.

2. The objected Specification and claims 48-62 are withdrawn.

3. Claim 43 was rejected under 35 U.S.C. 112, 1st paragraph is now

withdrawn.

4. Claims 1-7, 14-19, 23-30, and 37-63 remains rejected under 35 U.S.C.

102(e).

5. Claims 8-13, 20-22, and 31-36 remains rejected under 35 U.S.C. 103(a).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102

that form the basis for the rejections under this section made in this Office

action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act

of 1999 (AIPA) and the Intellectual Property and High Technology Technical

Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting

directly or indirectly from an international application filed before November 29, 2000.

Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

6.   Claims 1-7, 14-19, 23-30, and 37-63 are rejected under 35 U.S.C. 102(e) as being unpatentable over Coile, et al. (US 6,108,300).

As per claims 1 and 16:

Coile, et al. teaches method for providing a failover for a variety of network devices **300,310** such as firewalls (col.5, lines 7-12) in a network wherein the network includes servers **210,220** and a network flowswitch in the form of a failover cable **230** (col.5, lines 43-44).

Coile fails to point out that the network includes plurality of firewalls. However, Coile did suggest examples of the variety of network devices, which includes firewalls (col.5, lines 7-12). Therefor, it is inherent that plurality of firewalls includes in Coile's invention, so when a failure does occur, there is another firewall to take the place of the unoperational (failed) firewall to continuously protect the network from harmful intruders. Further, there exists a primary server **210**, a backup server **220**, a primary network device **300**, and a secondary network device **310** (col.6, lines 44-45). The failover cable determines the status of the servers (col.5, lines 43-48) and the failures of the network devices (col.6, lines 14-22). The network device periodically exchanges confirmation messages along the failover cable via the network to indicate that the network has not failed or a sends a failure message indicating the network device has failed (col.6, lines 43-67). Once a failure is detected, an active MAC

address of a functional backup network device is adopted and the MAC address of the failed network device is no longer in use (col.5, lines 55-58). Thus (the Examiner asserts), prevents the packets from being relayed to the failed network device, therefore, the packets are relayed to the functional network device with the active MAC address. The Examiner further asserts that each of the firewalls have a different fixed MAC address so when one firewall fails, it is directed to the active firewall therefore adopting the MAC address of the active firewall.

As per claim 2: See col.5, lines 26-31 discussing the plurality of servers.

As per claim 3:

Coile discuss each switch is associated with each connection where different network devices is connected at different ports (col.10, lines 32-43). Therefore, it is inherent to relay the packets to the functional firewalls over unshared ports so that packets can be forwarded to the standby device without confusion of which network device location has failed (col.10, lines 26-30).

As per claim 4: See col.6, lines 16-20 discussing sending confirmation messages to indicate it has not failed.

As per claims 5: See col.11, lines 2-8 discussing the ARP request.

As per claim 6:

Coile suggests ARP but fails to describe the functions of an ARP in more detail. The Examiner asserts the use of ARP request is to determine the physical address of a node. The Examiner asserts it is inherent the function of

an ARP request of Coile's invention is to find out the new address of the

functional firewall (col.12, lines 42-44). Therefore, Coile inherently teaches

responding to the ARP requests with an active MAC address of a firewall.

As per claim 7:

Coile teaches the use of the PING test during a 5 seconds interval to

determine if the remote device has failed (col.11, lines 10-25). The Examiner

asserts that Coile suggests the ICMP. As understood by the Examiner, Ping is

to see whether the machine is connected to a destination such as the Internet

and ICMP communicates errors and informs machines about an unreachable

destination. Therefore, the ICMP method for determining whether the

particular destination is reachable or operational.

As per claim 14: See col.6, lines 14-19 discussing transferring the packets

between the server and a firewall.

As per claim 15: See col.13, line 8.

As per claim 16:

Coile, et al. teaches method for providing a failover for a variety of

network devices **300,310** such as firewalls (col.5, lines 7-12) in a network

wherein the network includes servers **210,220** and a network flowswitch in the

form of a failover cable **230** (col.5, lines 43-44).

Coile fails to point out that the network includes plurality of firewalls.

However, Coile did suggest examples of the variety of network devices, which

includes firewalls (col.5, lines 7-12). Therefor, it is inherent that plurality of

firewalls includes in Coile's invention, so when a failure does occur, there is another firewall to take the place of the unoperational (failed) firewall to continuously protect the network from harmful intruders. Further, there exists a primary server **210**, a backup server **220**, a primary network device **300**, and a secondary network device **310** (col.6, lines 44-45). The failover cable determines the status of the servers (col.5, lines 43-48) and the failures of the network devices (col.6, lines 14-22). The network device periodically exchanges confirmation messages along the failover cable via the network to indicate that the network has not failed or a sends a failure message indicating the network device has failed (col.6, lines 43-67). Once a failure is detected, an active MAC address of a functional backup network device is adopted and the MAC address of the failed network device is no longer in use (col.5, lines 55-58). Thus (the Examiner asserts), prevents the packets from being relayed to the failed network device, therefore, the packets are relayed to the functional network device with the active MAC address. The Examiner further asserts that each of the firewalls have a different fixed MAC address so when one firewall fails, it is directed to the active firewall therefore adopting the MAC address of the active firewall.

As per claim 17: See col.11, lines 2-8 discussing the ARP request.

As per claim 18: See col.6, lines 16-20 discussing sending confirmation messages to indicate it has not failed.

As per claim 19: See col.13, line 8.

As per claim 23:

Coile, et al. teaches method for providing a failover for a variety of network devices **300,310** such as firewalls (col.5, lines 7-12) in a network that is coupled to the backbone of the Internet (col.12, line 65 – col.13, line 4). The network includes servers **210,220** and a switch circuit in the form of a failover cable **230** (col.5, lines 43-44). Coile fails to point out that the network includes plurality of firewalls. However, Coile did suggest examples of the variety of network devices, which includes firewalls (col.5, lines 7-12). Further, it is inherent that plurality of firewalls includes in Coile's invention, so when a failure does occur, there is another firewall to take the place of the unoperational (failed) firewall to continuously protect the network from harmful intruders. Further, there is MAC address for each primary server **210**, a backup server **220**, a primary network device **300**, and a secondary network device **310** (col.6, lines 44-45). The failover cable determines the status of the servers (col.5, lines 43-48) and the failures of the network devices (col.6, lines 14-22). The network device periodically exchanges confirmation messages along the failover cable via the network to indicate that the network has not failed or a sends a failure message indicating the network device has failed (col.6, lines 43-67). Once a failure is detected, an active MAC address of a functional backup network device replaces the MAC address of the failed network device (col.6, line 67 thru col.7, line 9). Thus (the Examiner asserts), prevents the packets from being relayed to the failed network device, therefore,

the packets are relayed to the functional network device with the active MAC address.

As per claim 24: See col.5, lines 26-31 discussing the plurality of servers.

As per claim 25: See col.12, lines 10-41 discussing the failover cable relaying the packet to the second firewall with a fixed MAC address.

As per claim 26:

Coile discusses the network device periodically exchanges confirmation messages along the failover cable via the network to indicate that the network has not failed or a sends a failure message indicating the network device has failed (col.6, lines 43-67).

As per claim 27: See col.11, lines 2-8 discussing the ARP request.

As per claim 28: See col.6, lines 16-20 discussing sending confirmation messages to indicate it has not failed.

As per claim 29: See col.11, lines 3-8 discussing monitoring responses.

As per claim 30:

Coile discusses that once a failure is detected, an active MAC address of a functional backup network device replaces the MAC address of the failed network device (col.6, line 67 thru col.7, line 9). Thus (the Examiner asserts), prevents the packets from being relayed to the failed network device, therefore, the packets are relayed to the functional network device with the active MAC address.

As per claim 37:   See col.6, lines 14-19 discussing transferring the packets between the server and a firewall.

As per claim 38: See col.7, lines 35-52 discussing full duplex between the firewall and the server.

As per claim 39: See col.13, line 8.

As per claim 40:

Coile, et al. teaches method for providing a failover for a variety of network devices **300,310** such as firewalls (col.5, lines 7-12) in a network wherein the network includes servers **210,220** and a network flowswitch in the form of a failover cable **230** (col.5, lines 43-44). Coile fails to point out that the network includes plurality of firewalls. However, Coile did suggest examples of the variety of network devices, which includes firewalls (col.5, lines 7-12). The failover cable is plugged on each side of the firewalls (col.7, lines 35-52) and the network device periodically exchanges confirmation messages along the failover cable via the network to indicate that the network has not failed or a sends a failure message indicating the network device has failed (col.6, lines 43-67). Once a failure is detected, an active MAC address of a functional backup network device replaces the MAC address of the failed network device (col.6, line 67 thru col.7, line 9). Coile fails to suggest sending a request message to a second side of the firewall. It is inherent if Coile can send a request message through the firewall by having the MAC address, then it is possible to send a

request message by using the MAC address to get to the location or to any side

of the firewall. See Fig. 1

As per claim 41: See col.13, lines 12-21 and FIG.9 discussing the first

memory and the second memory.

As per claim 42: See col.13, lines 12-21 discussing each session between

computers.

As per claim 43:

Coile, et al. teaches method for providing a failover for a variety of

network devices **300,310** such as firewalls (col.5, lines 7-12) in a network

wherein the network includes servers **210,220** and a network flowswitch in the

form of a failover cable **230** (col.5, lines 43-44). Coile fails to point out that the

network includes plurality of firewalls. However, Coile did suggest examples of

the variety of network devices, which includes firewalls (col.5, lines 7-12). The

failover cable is plugged on each side of the firewalls (col.7, lines 35-52) and the

network device periodically exchanges confirmation messages along the failover

cable via the network to indicate that the network has not failed or a sends a

failure message indicating the network device has failed (col.6, lines 43-67).

Once a failure is detected, an active MAC address of a functional backup

network device replaces the MAC address of the failed network device (col.6,

line 67 thru col.7, line 9). Coile fails to suggest sending a request message to a

second side of the firewall. It is inherent if Coile can send a request message

through the firewall by having the MAC address, then it is possible to send a

request message by using the MAC address to get to the location or to any side

of the firewall. See Fig. 1

As per claim 44: See col.6, lines 43-59 discussing the failover cable generates,

sends, and processes.

As per claim 45:

Coile teaches the use of NAT where the invention of Coile translates the

packet addresses (col.5, lines 60-61).

As per claim 46: See col.10, lines 39-42 discussing receiving and replying a

request on a port.

As per claim 47:

Differs from claim 23, wherein the network includes a second switch

circuit (col.10, lines 30-34).

As per claim 48: See col.12, lines 25-27 discussing the plurality of first

computers couple to the failover cable and its MAC address.

As per claim 49: See col.5, lines 55-58 discussing the second computers.

As per claim 50: See col.5, lines 44-45.

As per claim 51:

Coile discloses a flash memory device for storing programs or data

(col.13, lines 13-14). It is inherent that a memory can have multiple storage

elements to store the different data needs.

As per claim 52: See col.6, lines 43-59 discussing detecting and sending request message to the firewalls wherein the absence of the confirmation message indicates it has failed.

As per claim 53:

Coile discloses request message by ping and ARP methods, however, Coile fails to particularly suggest ICMP, for ICMP is similar to the ping method but differs that it performs error correction. The Examiner asserts that both methods are used to determine whether a destination can be reached and provides the status of the firewalls.

As per claim 54:

Coile discloses changing address portion of a packet when the backup server is active (col.12, lines 24-32). Otherwise, the Examiner asserts the packet will resume the original address and that it is not necessary to modify the packet if the first firewall is functional.

As per claim 55: See col.12, lines 15-22 discussing replacing each received packet with the fixed MAC address of a functional firewall.

As per claim 56: See col.6, lines 2-3.

As per claim 57:

Coile, et al. teaches method for providing a failover for a variety of network devices **300,310** such as firewalls (col.5, lines 7-12) in a network. Coile fails to point out that the network includes plurality of firewalls. However, Coile did suggest examples of the variety of network devices, which

includes firewalls (col.5, lines 7-12). The network device periodically exchanges confirmation messages along the failover cable via the network to indicate that the network has not failed or a sends a failure message indicating the network device has failed (col.6, lines 43-67). Once a failure is detected, an active MAC address of a functional backup network device replaces the MAC address of the failed network device (col.6, line 67 thru col.7, line 9). See Fig.1

As per claim 58: See col.7, lines 36-52 discussing the switch circuit performs detection.

As per claim 59: See FIGURES 8 and 9.

As per claim 60: See FIGURE 4 transferring the packets through a switch circuit.

As per claim 61:

Coile discloses a method of taking over the active IP address of the formerly active device that was deemed a failure. Therefore it is inherent that Coile does not change the IP address during the transferring of the packets to any of the firewalls. See col.12, lines 29-31.

As per claim 62:

The Examiner asserts it is inherent that Coile does not change the IP address during the transferring of the packets to any of the firewalls. See col.12, lines 29-31.

As per claim 63: See col.5, lines 55-65.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7.   Claims 8-13, 20-22, and 31-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coile, et al. and further in view of Belville, et al. (US 5,828,833).

As per claim 8:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17).

As per claim 9:

As rejected in claim 8, and further includes where Belville discusses the cleanup thread including waiting for a time out period to pass (col.6, lines 56—63). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because when the time out passes the privileges are allocated so the packet is not transferred to the non-operational firewall.

As per claim 10:

The same rationale applies to claim 9, and further includes the time out period is greater than or equal to a time period needed for the recovered firewall to learn routes to all the known clients. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because it is more secure by having the advantage to have enough time and not less than the time period to learn the routes to all known clients. Else, there is no point for the recovered firewall to operate as securely as before. See col.5, lines 3-9 and col.12, lines 47-53.

As per claim 11:

The same rationale applies of claim 8, and further includes where Belville discusses periodically pinging the firewall application to see if it is still operational. The Examiner asserts if the failed firewall receives a ping and responds, then that is an indication the firewall has recovered and is functional once again. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because it is an indication that the firewall has regained its operational state. See col.6, lines 36-55.

As per claim 12:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the

system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17). Also, see col.9, lines 3-17.

As per claim 13:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17). See col.6, lines 36-55.

As per claim 20:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17).

As per claim 21:

The same rationale applies of claim 20, and further includes where Belville discusses periodically pinging the firewall application to see if it is still operational. The Examiner asserts if the failed firewall receives a ping and responds, then that is an indication the firewall has recovered and is functional once again. Therefore, it would have been obvious to one of ordinary skill in

the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because it is an indication that the firewall has regained its operational state. See col.6, lines 36-55.

As per claim 22:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17). See col.6, lines 36-55.

As per claim 31:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17).

As per claim 32:

As rejected in claim 8, and further includes where Belville discusses the cleanup thread including waiting for a time out period to pass (col.6, lines 56—63). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the

system of Coile, because when the time out passes the privileges are allocated so the packet is not transferred to the non-operational firewall.

As per claim 33:

The same rationale applies to claim 32, and further includes the time out period is greater than or equal to a time period needed for the recovered firewall to learn routes to all the known clients. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because it is more secure by having the advantage to have enough time and not less than the time period to learn the routes to all known clients. Else, there is no point for the recovered firewall to operate as securely as before.   See col.5, lines 3-9 and col.12, lines 47-53.as rejected on the same basis as claim 10.

As per claim 34:

The same rationale applies of claim 31, and further includes where Belville discusses periodically pinging the firewall application to see if it is still operational. The Examiner asserts if the failed firewall receives a ping and responds, then that is an indication the firewall has recovered and is functional once again. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because it is an indication that the firewall has regained its operational state. See col.6, lines 36-55.

As per claim 35:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17). See col.6, lines 36-55.

As per claim 36:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no

response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention were made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17).

Minor Informalities

8.   *Claim 51 is objected to because of the following informalities:*

On line 6, the word "identify" should be "identity".

Appropriate correction is required.

Response to Argument

A thorough review of the prior art (Coile, Et Al.) proves that each of the firewalls have a "fixed" MAC address. The Examiner asserts that each firewall would have a fixed address and not a type of firewall where the MAC address would constantly change; the only change would be the packets. It would not be logical if the failed firewall takes on an address of an active firewall leaving that firewall that is really active with no responsibilities. Then the packets would still becoming to a failed firewall thinking it is going to an active firewall because of the active MAC address. The Examiner ascertains that once a firewall has failed the MAC address is no longer valid and the system would switch over to a firewall that is active in order to process the all the packets.

Coile teaches that upon detection of the failed firewall, the packet will

"adopt" the MAC address of the active firewall. According to claim 1 on lines 8-

15, states that to detect the packet directed to the failed firewall and changing

the MAC address to an active firewall's address (col.5, lines 55-57). Coile does

teach this on col.5, lines 57-60; where it intercept the packets and translates

the packet addresses meaning changing the MAC address to the active MAC

address of a functional firewall.

Please refer to Coile, Et Al. on col.5, Et SEQ. for more details concerning

the rejections above.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension

of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire

THREE MONTHS from the mailing date of this action. In the event a first reply

is filed within TWO MONTHS of the mailing date of this final action and the

advisory action is not mailed until after the end of the THREE-MONTH

shortened statutory period, then the shortened statutory period will expire on

the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In

no event, however, will the statutory period for reply expire later than SIX

MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (703) 305-3853. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5631.

Lha

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100